United Nations E/CN.15/2001/4

Economic and Social Council

Distr.: General
30 March 2001

Original: English

Commission on Crime Prevention and Criminal Justice
Tenth session
Vienna, 8-17 May 2001
Item 4 of the provisional agenda*
International cooperation in combating transnational crime

Conclusions of the Study on effective measures to prevent and control high-technology and computer-related crime

Report of the Secretary-General

Summary

The present report responds, in part, to the request of the Economic and Social Council, in its resolution 1999/23 of 28 July 1999, that the Secretary-General conduct a study on effective measures that could be taken at the national and international levels to prevent and control computer-related crime. It provides a preliminary examination of the subject and recommends that a more detailed study be undertaken and submitted for consideration by the Commission on Crime Prevention and Criminal Justice at its eleventh session as a matter of high priority. It further recommends that the Commission at its eleventh session consider a series of options for further action, including the possible drafting of an international instrument against computer-related crime and options for a shorter-term strategy, including the establishment of a United Nations global programme against high-technology and computer-related crime. It also provides information about the activities of other relevant international and intergovernmental organizations and seeks to respond to some of the concerns raised by individual Member States.

* E/CN.15/2001/4.

V.01-82399 (E) 250401 260401

Contents

		Paragraphs	Page
I.	Introduction	1	3
II.	Background	2-34	3
	A. Consideration by other intergovernmental or international organizations	2-12	3
	B. Activities of the United Nations	13	5
	C. The nature of computer-related and high-technology crime: a preliminary typology	14-29	7
	D. Assessing the scope and costs of computer-related and high-technology crime	30-34	9
III.	Conclusions and recommendations: the development of global policies for the prevention and control of computer-related and high-technology crime	35-55	11
	A. The need to treat high-technology and computer-related crime as a distinct subject	35	11
	B. The need to assist developing countries	36-39	11
	C. The need to consider international, national and private-sector measures	40-41	12
	D. The role of the United Nations	42-49	12
	E. Elements of a detailed study	50	14
	F. Options and specific recommendations for further work on high-technology and computer-related crime	51-55	15

I. Introduction

1. The problem of criminal activity involving modern computer, computer-network and telecommunications technologies continues to represent a significant challenge to the criminal justice and law-enforcement communities of Member States. That challenge can be seen as having the following distinct elements:

(a) The challenge is global. In the past, most of the users of modern technologies, and hence most of the offenders and victims, have been located in developed countries. The extension of access to developing countries has been identified as a major priority, in order to ensure that the global information society becomes a factor that supports development rather than a further obstacle to it.[1] Developing countries will be vulnerable to computer and telecommunications crime and could be excluded from access to computer and communications networks by crime prevention or security technologies if they are not able to participate in the development and implementation of crime-control policies;

(b) The challenge is dynamic. The rapid development of new technologies results in an equally rapid development of criminal innovations, and the global nature of the technologies results in the rapid spread of new criminal techniques. Monitoring both legitimate development and criminal innovation in order to keep domestic and international responses up to date will therefore be critical, in particular in countries where technical resources are limited. The process is primarily driven by technological development, and is therefore open-ended;

(c) The challenge is multidisciplinary. The development of computer and telecommunications network technologies underlies a major shift from social and economic activities involving physical exertion and commodities to those involving pure information or knowledge. That raises major implications in fields such as human rights and sustainable social and economic development. It will be important for crime control to become an element of those agendas, and vice versa. Information technologies and the architecture of computer and telecommunications networks are also largely the products of private-sector development, and the development of measures against high-technology and computer-related crime must take into consideration factors such as commercial viability and the economic competitiveness of the technologies involved.

II. Background

A. Consideration by other intergovernmental or international organizations

2. The growing concern of States about the nature and extent of the problem and the need for effective global measures against it is evidenced by the number of forums in which it has been considered.

1. The Council of Europe

3. The Council of Europe is nearing completion of the text of a Convention on Cyber-crime,[2] which will deal with criminal offences relating to interference with systems, unauthorized access, electronic fraud and forgery, offensive content and intellectual property offences. The draft text deals with investigative powers, including the tracing of communications and the search for and seizure and preservation of electronic evidence. It will also define basic terms and set standards for mutual legal assistance and other forms of international cooperation. When successfully completed, it will represent the first attempt at a comprehensive international instrument against computer-related crime. The completed draft text has met with a mixed reception. Generally, Governments, experts and law-enforcement agencies see it as a positive development, although many feel that some of the more difficult issues have not been addressed. Many interest groups take the position that international networks should not be regulated, and have attacked the instrument as an attempt to extend domestic law enforcement powers at the expense of individual privacy and other interests.

4. The negotiations on the text of the instrument were conducted by a Committee of Experts on Crime in Cyberspace, established in February 1997 following several earlier studies of the problem.[3] In addition to regular members of the Committee, experts from Canada, Japan and the United States of America were invited to participate in its proceedings, and other States joined the process during the course of

negotiations. The Committee produced 25 successive draft texts during the term of its mandate, which concluded in December 2000. The final text has been submitted to the Parliamentary Assembly of the Council of Europe. It will subsequently be submitted to the European Committee on Crime Problems for review in June 2001, and, if approved, would then be transmitted to the Committee of Ministers of the Council of Europe for adoption.

2. The Group of 8

5. Following discussions about the problems arising from transnational crime at its summit meeting held in Halifax, Canada, in June 1995, the seven major industrialized countries and the Russian Federation (Group of 8) established the Lyon Group of Senior Experts on Transnational Organized Crime, which included a subgroup of experts on computer-related crime. The subgroup has met regularly since 1997 and produced a number of initiatives. The major concerns that it examined were the problems posed by cross-border electronic searches, the tracing of communications and the need for cooperation between Governments and relevant private-sector interests.

6. In December 1997, the Group of 8 adopted a 10-point action plan on cybercrime that included the review of legislation, measures to ensure the availability of trained and equipped law enforcement personnel, the consideration of cybercrime issues when negotiating legal assistance agreements, consideration of methods for preserving electronic evidence and making it available in foreign criminal proceedings, better cooperation with industries and forensic and other technical standards for computer security and the use of electronic evidence in legal proceedings.[4]

7. In 1999, the Group of 8 adopted some preliminary basic principles for law enforcement agencies seeking access to electronic data stored in foreign States.[5] In general, it agreed that data could be freely accessed if publicly available, as would be the case on an open web site, for example, or where the consent of a person with lawful authority to access and disclose the data was obtained. For data not publicly available, searchers face a dilemma. If they do not copy the data quickly, offenders will usually erase it. If they do copy it without first asking the permission of the State in which it is located, serious issues arise with respect to the sovereignty of that State and the protection of the rights of persons with an interest in the data being seized. The principles agreed upon by the Group of 8 involve a request for expedited mutual legal assistance. The State in which the data are located would be asked to take immediate steps to preserve them pending more formal assistance to ensure their seizure and disclosure to the requesting State. The transfer of the data to the requesting State would then be accomplished using more conventional proceedings and safeguards for mutual legal assistance.

8. Also under consideration are basic principles for the tracing of communications on computer networks. Electronic records of the source and destination of communications such as electronic mail are kept by most service providers, but only for limited periods of time. Records that can be used to trace communications and identify the system users involved can in most countries only be accessed using judicially reviewed search and seizure operations. That does not pose a serious obstacle to tracing most domestic communications, but in transnational cases the delays are increased by the additional need to make requests through mutual legal assistance channels. That problem is known to sophisticated offenders, who exploit it by routing their communications through large numbers of different countries between source and destination, or routing them through countries that lack the laws or infrastructure to conduct successful traces in order to conceal the true origin or destination of their communications.

9. To facilitate fast cooperation between law enforcement agencies in transnational cases, the Lyon Group recommended the establishment of a network of contacts in each State who could be called upon 24 hours a day, seven days a week, to provide competent investigative assistance. The network initially consisted of States members of the Group of 8, but it has now been expanded to include 19 countries and operational responsibility has been transferred to the International Criminal Police Organization (Interpol).

10. To bring together Government and private-sector interests, the Group of 8 has held several conferences on cooperation with industry.[6] In general, industry representatives include companies that develop computer and telecommunications hardware, software and other infrastructure elements and those that provide services to individual users. The discussions have considered issues relating to the willingness and ability

of companies to cooperate with law enforcement and the need for crime prevention through customer education and the incorporation of security elements into new, developing technologies.

3. Other international or intergovernmental organizations

11. The question of high technology and computer-related crime has also been taken up by other intergovernmental and international organizations, both as a distinct topic and in the context of other crime-related considerations such as money-laundering and transnational organized crime. The Commonwealth began examining those questions in 1998, placing the subject on the agenda of a meeting of the Commonwealth Law Ministers in May 1999. That meeting established a working group of experts on computer and computer-related crime to draft model legislation for Commonwealth countries, but deferred work on the project until the conclusion of the Council of Europe Convention on Cyber-crime. Work resumed in July 2000 and draft model legislation is being prepared. The Commonwealth also undertook to circulate materials on international developments to its member States, and to review Commonwealth schemes dealing with fugitive offenders and mutual legal assistance to ensure that such schemes would extend the necessary forms of cooperation to the new field of high-technology crime.

12. Interpol has also become active, establishing a series of regional working parties on information technology crime. The research conducted and materials produced by Interpol have tended to reflect the needs and concerns of law enforcement. Materials for use in training investigators include a handbook for novice investigators and a more elaborate computer crime manual setting out best practices and techniques for advanced investigators. Interpol is also aware of the need to use high-technology media to disseminate information to law enforcement agencies and is establishing a web site for that purpose. It has assumed responsibility for maintaining an up-to-date directory of the network of contacts originally established by the Lyon Group. Interpol plans further activities, in particular in the area of law enforcement training, and will monitor or participate in the activities of other international organizations to share information and avoid duplication of effort.

B. Activities of the United Nations

13. The issue of crime involving computer and telecommunications technologies has been addressed in the activities of the United Nations and remains under active review. In addition to the present study, conducted pursuant to Economic and Social Council resolution 1999/23 of 28 July 1999,[7] the following action has been taken to deal with that issue:

(a) In General Assembly resolution 45/109 of 14 December 1990 and Economic and Social Council resolution 1996/11 of 23 July 1996, Member States are urged to employ modern computer technologies for the more effective and efficient administration of criminal justice operations and information systems. The Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held in Havana from 27 August to 7 September 1990, recommended the development of an international instrument dealing with the computerization of criminal justice systems.[8] The matter was taken up at a two-day workshop held during the Ninth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held in Cairo from 29 April to 8 May 1995, which noted that there was a need for computerization in order to keep pace with new forms of crime, but that there were concerns about privacy, human rights and the interoperability of systems within and between countries. The workshop also noted the need for technical assistance in the form of both financial resources and technical expertise.[9] In general, the process focused on the use of computers in the administration of criminal justice and the gathering of statistical information, rather than on the use of computer networks as an investigative or operational tool. More recently, provisions to enhance the use of modern technologies in crime control were incorporated into the United Nations Convention against Transnational Organized Crime,[10] and the electronic distribution of documents played an important role in the negotiation process;

(b) The Eighth Congress also considered the problem of computer-related crime itself,[11] recommending a series of measures relating to:

(i) The modernization of domestic offences, investigative procedures, rules of evidence, forfeiture or restitution, mutual legal assistance and extradition provisions, in order to ensure their

extension to cases involving computer-related crime;

(ii) The improvement of computer security and other technical measures for crime prevention;

(iii) The education of members of the public and the training of officials in the investigation, prosecution and adjudication of cases involving computer-related crime;

(iv) The development and dissemination of rules of ethics in the use of computer systems;

(v) The development of policies for dealing with victims of computer-related crime, including measures to encourage the reporting of such crimes;

(c) As recommended by the Eighth Congress in its resolution 9, the *United Nations Manual on the Prevention and Control of Computer-related Crime* was published in 1994[12] as a resource for investigators and policy makers, and has been made widely available on the Internet;

(d) The question of computer-related crime was also included in the agenda of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held in Vienna from 10 to 17 April 2000. During the Tenth Congress, a one-day workshop on the subject was organized by the United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders.[13] The workshop consisted of four panel discussions on the following topics: the criminology of computer-related crime; problems associated with search and seizure on computer networks; problems associated with the tracing of communications on computer networks; and the relationships between law enforcement agencies and the computer and Internet industries. Leading experts in the field briefed participants on current issues and progress in discussions in the Council of Europe, the Group of 8 and other forums. In addition to the representatives of participating States, several industry representatives participated. The workshop made several recommendations, including calls for greater cooperation between Governments and industry, improved international cooperation in tracing offenders and further action by the United Nations regarding the provision of technical cooperation and assistance;[14]

(e) The Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century, adopted by the Tenth Congress[15] and endorsed by the General Assembly in its resolution 55/59 of 4 December 2000, also dealt with high-technology and computer-related crime. In paragraph 18 of the Vienna Declaration, Member States decided to develop action-oriented policy recommendations on the prevention and control of computer-related crime, and committed themselves to working towards enhancing their ability to prevent, investigate and prosecute such crime. The Commission on Crime Prevention and Criminal Justice was invited to undertake the development of those policy recommendations, taking into account work already under way in other forums. The General Assembly, in its resolution 55/60 of 4 December 2000, subsequently requested the Commission to continue its consideration of the findings and recommendations embodied in the Vienna Declaration and the report of the Tenth Congress, and requested the Secretary-General, in consultation with Member States, to develop draft plans of action for consideration by the Commission at its tenth session;

(f) In addition to its involvement in the preparation of the workshop held during the Tenth Congress on crimes related to the computer network, the United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders has conducted a series of meetings and workshops to identify issues and set an agenda for subsequent activities. It has conducted a survey of Member States on issues involving computer-related crime, the results of which are forthcoming. It is also currently engaged in compiling and publishing the materials used by the United Nations and individual participants in the workshop held during the Tenth Congress. Its future plans centre around the development and dissemination of practical information for the investigation and prosecution of computer-related crime;

(g) The Commission, at its tenth session, will have before it a report of the Secretary-General on the draft plans of action for the Implementation of the Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century (E/CN.15/2001/5). The report of the Secretary-General also deals with high-technology and computer-related crime and includes a series of policy recommendations and specific measures that could be undertaken to enhance the capability, at domestic and international levels, to

prevent, investigate and prosecute such crime. Those recommendations and measures are based on the material dealt with in the present report;

(h) The General Assembly, in its resolution 55/63 of 4 December 2000, takes note of the value of efforts to combat the criminal misuse of information technologies. Such efforts would include the following: elimination of safe havens for offenders; law enforcement cooperation on international cases; exchange of information; training and equipping of personnel; protection of confidentiality; preservation of and quick access to data pertaining to criminal investigations; maintaining adequate mutual legal assistance regimes; raising public awareness of the problem; designing information systems to prevent crime and facilitate its investigation; and taking into account the need to protect individual freedoms and privacy while preserving the capacity of Governments to fight criminal misuse of information technologies. The Assembly also decided to maintain the question of the criminal misuse of information technologies on the agenda of its fifty-sixth session;

(i) By its resolution 55/25 of 15 November 2000, the General Assembly adopted the United Nations Convention against Transnational Organized Crime and two protocols thereto (resolution 55/25, annexes I-III). The Convention does not apply in cases where the offences involved are not serious crimes, where there is no involvement of an organized criminal group, or where there is no element of transnationality in any of the offences involved,[16] which would exclude some electronic offences. It would apply, however, where computer or telecommunications networks are used by offenders in support of more traditional forms of transnational organized crime. Article 29, paragraph 1 (h), specifically calls for the development of domestic measures and technical assistance to combat transnational organized crime committed through the use of computers, telecommunications networks or other forms of modern technology;

(j) Following the adoption of the Convention, a further workshop on the theme "The Challenge of Borderless Cybercrime" formed part of the Symposium on the Rule of Law in the Global Village—Issues of Sovereignty and Universality, conducted within the framework of the High-level Political Signing Conference for the United Nations Convention against Transnational Organized Crime and the Protocols Thereto, held in Palermo, Italy, from 12 to 15 December 2000. The topics dealt with included computer-related crime and other forms of transnational criminality for which controls rooted exclusively in domestic law were increasingly seen as inadequate. It was noted that such crime was expanding with the proliferation of the technologies on which it relied and as the commission of cross-border offences became easier. Legislation at the national level and a comprehensive international instrument were seen as important elements of a solution, but there were also concerns about the danger of developing regulations prematurely. The problem could also be addressed in part by prevention using such things as technical security, education and the development of ethical standards for the use of new technologies. The workshop also suggested that the range of cybercrimes could be broken down into the following basic categories: unauthorized access to computers or computer systems; destruction or alteration of data; interference with lawful use of computers or computer systems; theft of intangible property; and obtaining value by deception.

C. The nature of computer-related and high-technology crime: a preliminary typology

14. The phenomenon of high-technology and computer-related crime requires the identification of entirely new offences and the modification of existing offences to ensure that they extend to misuses of the new technologies. New forms of harmful conduct have had to be examined with a view to determining whether the application of the criminal law is appropriate as a response, and whether the conduct involved should be made a crime at all. International consensus is emerging with respect to a substantial core of the most serious and harmful conduct, but some areas remain which are treated as crimes by some States but not all. The two major examples are intellectual property problems, such as the unauthorized copying of software or data, and the problem of what is described as offensive content.

15. Criminal exploitation of the new technologies has resulted in entirely new forms of crime. In other cases, more traditional forms of crime are committed in new ways that increase benefits or reduce risks to offenders. A third basic category of criminal activity consists in

the more general use of the technologies by offenders to organize, to communicate, and to shield their activities from surveillance. Other basic fields of classification proposed include classification according to whether the crimes are committed for economic or material gain for offenders or other motives, and whether the offences involve crimes committed against computer or communications systems or the use of those technologies to victimize others.

16. Basic types of high-technology and computer-related crime are described below.

1. Crimes committed against the technologies and their users

(a) Gaining unauthorized access to computers or computer systems

17. In most cases, gaining unauthorized access to computers or computer systems is treated as a crime out of concern for invasion of the privacy of legitimate users whose data may be accessed, and because unauthorized access often accompanies other offences or interferes with legitimate use of the system.

(b) Unauthorized use of computer systems

18. Unauthorized use of computer systems overlaps with unauthorized access, since systems must be used to gain such access. Once access is gained, however, systems are also used to commit other offences or to conceal the true identity of the offender. Unauthorized use is usually made a crime on the grounds that use of computer time or facilities represents a valuable commodity that is not paid for by the offenders and that is in some cases denied to legitimate, fee-paying users.

(c) Reading, copying or taking data without authorization

19. As with conventional theft, the harm of reading, copying or taking data without authorization consists in the loss of value to the victim and an improper gain of value on the part of the offender. In the case of data, however, those aspects are separate, as data can be copied without removing them. Such an act may also be criminalized as a form of invasion of privacy.

(d) Creating or propagating hostile programs

20. Computer viruses, worms and other programs interfere with system operations by consuming computing and storage capacity. In most cases, they also propagate themselves using e-mail or the transfer of contaminated diskettes, so that offenders quickly lose control over the scope of the damage caused once the program has been released. Many hostile programs also inflict actual damage on data, erasing or distorting files. The harm, which can be substantial, consists in the loss of system operations, the loss of valuable data and the cost of removing the programs and restoring system functions.

(e) Computer vandalism or sabotage

21. Damage can be done directly by offenders who have gained unauthorized access, either intentionally or unintentionally, while attempting to use the system or conceal the fact that access has been gained. Such offences are also committed in some cases by insiders who have authorized access to the system involved. The category includes denial-of-service attacks, in which the offender gains unauthorized access to a large number of networked computers and uses them to bombard the target system with random data, overloading the target and causing it to shut down. That may constitute simple vandalism or be used as a diversion to conceal other offences by disabling technical security mechanisms. Hostile programs such as viruses can also be used for specific acts of vandalism or sabotage, but can be distinguished from the direct actions of offenders because, once they propagate, they usually act with indiscriminate effect.

2. Conventional crimes committed using computer or communications technologies

(a) Offences involving offensive content

22. Offences involving offensive content consist in the use of computer systems to produce or disseminate images, text or other information that is subject to criminal sanctions. There are discrepancies between the types of content criminalized in different States. Most States currently criminalize the creation or distribution of child pornography, but there is less consensus with respect to material viewed as obscene, pornographic or blasphemous or as hate propaganda. Protecting constitutional principles of human rights including freedom of expression or speech, limits the extent to which many States can criminalize some forms of content.

(b) Internet-related abduction

23. Paedophile offenders have begun to use the Internet as a way to gain access to children without

revealing their true identities. Dialogues are started in electronic chat rooms, and once confidence is gained, the offender arranges a personal meeting and abducts the victim. A number of offenders have been arrested by law enforcement officers posing as children on the Internet. In some cases, offenders have induced victims to delete files recording their conversations in order to conceal evidence of the abduction.

(c) Fraud

24. The category of fraud includes most crimes in which funds are electronically misdirected or in which technology users are given false information in order to deprive them of funds or asset value. Such offences may be committed by insiders such as employees, or by outsiders using unauthorized access to private systems or placing false information on public systems. Fraud and other economic offences are expected to increase significantly as electronic commerce expands. An increasing problem in this area is the use of the technologies to manipulate financial markets.

(d) Commercial or industrial espionage

25. The increasing reliance of companies on computer systems to create and transfer information has also made them targets for industrial espionage. Such espionage can be conducted by gaining unauthorized access from outside, or by insiders using the technologies to assemble valuable information and send it to competitors without detection.

(e) Intellectual property crimes

26. The ability of new technologies to store, transmit and copy information makes unauthorized copying and use a major area of concern. Not all States treat such actions as a criminal matter, however. Some deal with them as a civil matter between the parties directly involved.

(f) Gambling

27. The development of infrastructure to support small-scale electronic commerce has also made Internet gambling possible. The criminal law is involved when web sites in jurisdictions where gambling is legal are used by gamblers in jurisdictions where it is a crime. Apart from moral considerations, gambling is often regulated to generate tax revenues and to ensure oversight to exclude organized crime and protect gamblers from unfair play. More recently, Internet gambling is also seen as a possible means of conducting money-laundering operations.

(g) Money-laundering

28. The ongoing increase in electronic commerce and other commercial activity using computer networks is expected to open up numerous opportunities for money-laundering. Generally, the technologies allow offenders to conceal their true identities and locations, to exploit jurisdictional differences by using foreign accounts or multiple jurisdictions, and to conceal the true nature of their transactions using technologies such as encryption. In some cases, other crimes such as gambling or fraud may also be involved.[17]

3. Use of the technologies to support other criminal activities

29. In general, modern computer and telecommunications networks and other such technologies offer criminal organizations the same advantages that they offer to legitimate businesses. The advantages include fast, reliable, low-cost global communications that in most cases are more secure from outside interception or surveillance than more traditional methods. The nature of networks and the higher speeds and volumes of data being transferred make it inherently more difficult for law enforcement agencies to intercept individual communications. Dedicated security products such as firewalls and encryption software shield criminal communications from interception or intrusion just as effectively as they protect legitimate communications. Network technologies may also in some cases support entirely new forms of criminal organization. The most commonly cited example is paedophile offenders, who can locate one another and share child pornography while remaining anonymous, and may cooperate in ways not covered by existing concepts or definitions of organized crime. More conventional criminal organizations may also find new opportunities to identify and cooperate with offenders from other regions or countries.

D. Assessing the scope and costs of computer-related and high-technology crime

30. As computer and telecommunications networks have expanded in scope and sophistication, the number of people who use them and the degree of reliance

placed on them, have both increased dramatically. In a report to the Millennium Assembly of the United Nations, the Secretary-General noted that since its beginnings in the early 1990s, the Internet had reached 143 million users by 1998, and that 700 million were expected to be online by 2001. The value of electronic commerce, a more recent phenomenon, had reached a total of 2.6 billion United States dollars ($) by 1996, and was expected to top $300 billion by 2002.[18] There are few comprehensive statistics concerning high-technology or computer-related crime, but anecdotal evidence and such statistics as are available suggest that the extent of such crime is increasing with the growing number of potential offenders and victims online.[19] The range of criminal activities also appears to be expanding as technologies create new criminal opportunities and offenders find new ways to exploit them. Of particular concern currently is the rapid expansion of electronic commerce and its supporting infrastructure, which are likely to be accompanied by subsequent increases in economic computer-related crimes such as fraud, the manipulation of financial markets and money-laundering.

31. As the degree of reliance placed on networks increases, the potential harm from criminal offences also increases. Most industrialized countries, in which the reliance is greatest, now consider computer and telecommunications networks and their supporting infrastructure as potential targets for terrorism. Attacks on computer systems for strategic or political reasons are still rare, but criminal acts based on other motives regularly cause large-scale harm, in some cases out of all proportion to that actually intended by the perpetrators. Recent examples include the creation and propagation of the "Melissa" virus in March 1999, which caused over $10 million in direct damage in the United States alone, and the "I love you" virus in May 2000, estimated to have caused damage of between $7 billion and $10 billion and to have infected as many as 45 million computers worldwide. A further incident, a series of denial-of-service attacks, bombarded web sites with large volumes of meaningless data, shutting down 1,200 sites, including those of news organizations and electronic commerce sites, in less than two hours. Losses from some incidents, in particular involving viruses, are compounded in most cases when other offenders copy the virus, make changes to conceal its nature from users or filtering software, and then repropagate it.[20]

32. Actual losses are difficult to quantify, but include direct costs of repairing systems and software, the loss of access or services to users and consequent damage, the loss of valuable data and the loss of revenue from site operations. Such crimes also necessitate the development and maintenance of security and other preventive measures, an added cost factor. The overall increases in such crime and the spectacular nature of some of the offences involved also generate substantial but unpredictable political pressures for the enhancement of criminal law controls, more severe punishments and technical precautions on the part of the producers of software and hardware and of companies that provide network access to customers. A further hidden cost of such incidents is the fear of cybercrime, which may erode usage of the technologies or deter Governments and populations in developing countries from making the most effective use of them.

33. The search for reliable analysis of the nature and scope of the offences themselves is also difficult. Issues remain open with respect to whether some forms of conduct should be criminalized at all, and if so, how they should be defined and classified. Any classification system also depends in part on the technologies involved, which also raises definitional issues. Technologies such as computer networks, cable broadcasting systems and cellular and conventional telephone systems are rapidly becoming indistinguishable as the uses of computer networks expand and more traditional systems take up digital technologies. A current example of that is the so-called palm-pilot device, which combines aspects of cellular telephony, network broadcasting and access to computer networks. That will challenge researchers, policy analysts and legal drafters for the foreseeable future, and has led to calls for the use of technology-neutral concepts and language to ensure that gaps and inconsistencies are avoided.

34. The gathering of accurate statistics also presents problems even where the offences are clearly identified. Most experts believe that common forms of computer-related crime are significantly underreported because victims may not realize that they have been victimized, may not realize that the conduct involved is a crime, or may decide not to complain for reasons of embarrassment or corporate credibility. Further problems arise with the mass victimization caused by offences such as virus propagation, because the numbers of victims are simply too large to identify and count, and because such programs can continue creating new victims long after the

offenders have been caught and punished. A further factor complicating the gathering and comparison of national crime statistics will be the fact that transnational computer-related crimes are, by definition, committed in or have effects in at least two States, and, in some cases, in many States, risking multiple reporting or no reporting at all.

III. Conclusions and recommendations: the development of global policies for the prevention and control of computer-related and high-technology crime

A. The need to treat high-technology and computer-related crime as a distinct subject

35. The criminal activities considered in the present report are linked by underlying technologies and share many common characteristics. Some are new activities, created and defined by the technologies themselves, while others are more traditional forms of crime that have been substantially influenced by those technologies. Many fundamental policy issues, such as the striking of an appropriate balance between human rights and investigative powers and between domestic and international interests, are common to all forms of high-technology and computer-related crime. At a more practical level, the problems faced by investigators and prosecutors, such as locating and identifying offenders and the seizure, preservation, authentication and use of computer or electronic evidence in court, are substantially the same regardless of the nature of the offences themselves. It is therefore recommended that this area be treated as a distinct subject for the purposes of research and any future multilateral discussions. It should also be noted, however, that many emerging areas of concern, such as the dissemination of child pornography, fraud and other financial crimes, will also require the input of experts familiar with the offenders involved and their specific methods.

B. The need to assist developing countries

36. Much of the policy debate about computer systems and computer-related crime thus far has taken place within and among countries with well-developed high-technology sectors. Those countries have substantial interests that may be adversely affected by computer-related crime. They have extensive public- and private-sector investments in the technologies, as well as populations that rely increasingly on the use of computer networks. The interests of developing countries are also at issue, however. New technologies represent a major opportunity to advance the social, economic and other interests of developing countries,[21] but they could also aggravate existing disparities if those countries are not able to take full advantage of that opportunity. In that regard, both computer-related crime and the efforts of developed countries and high-technology industries to combat such crime may become an obstacle to development if developing countries cannot participate effectively in discussions. Their input is needed to identify and articulate their interests fully, to identify needs for technical and other assistance at various stages of the process, to develop measures for crime prevention and control that are viable in all societies, and to ensure the full and effective implementation of those measures.

37. Near-universal implementation of effective crime control measures will be needed because the new technologies can be exploited by criminals with virtually none of the restrictions imposed on traditional offenders by national borders. Where traditional offenders are limited by factors such as geographical distance, customs controls and the need for physical access to their victims, electronic offenders can operate remotely and with effective impunity from or through any jurisdiction that lacks adequate legislation or the will or capability to enforce such legislation. Broad representation and effective participation will be essential to ensuring that policies and measures developed are viable for all countries and that all countries are willing and able to implement them effectively.

38. Ensuring effective participation will require the assistance of developed countries at several stages of the process. At the outset, input from developing countries will be needed to assess their interests in the technologies themselves and how those interests may be affected by computer-related crime and efforts to control it. That makes assistance at the earliest stages particularly important. Some countries have been actively engaged for some time, but, for many, the technologies are still unfamiliar and there has not been

much consideration of the technical, legal and policy issues that will arise. Even with assistance, the development of such expertise takes time. It is therefore important that such assistance begin as quickly as possible and that it continue long enough to ensure effective participation as long as discussions take place. Over the longer term, ongoing technical assistance will also be needed to maintain operational effectiveness. The fact that the technologies and the offences that depend on them continue to evolve will require a global effort to monitor new developments, develop effective responses, and disseminate these quickly enough to keep law enforcement agencies and prosecutors abreast, if not ahead, of offenders.

39. It is therefore recommended that immediate efforts be made to assess the technical assistance needs of developing countries that request it and to meet those needs as quickly as possible. The assessment should be done in the context of the electronic development strategies of those countries and the increasing global use of technologies for computer and telecommunications systems and crime prevention. It should also be done in consultation with, and where possible with the assistance of, the private-sector companies responsible for the technologies. Important elements of the assessment in global terms will include the identification of critical technologies and the setting of priorities.

C. The need to consider international, national and private-sector measures

40. Experts universally recognize that the international character of modern computer and telecommunications technologies has led to new forms of transnational and multinational crime. The concept of cyberspace and the ease with which criminal acts in one geographic location can have effects in others makes the integration of national and international measures essential. Without such integration, countermeasures may be ineffective against crime, and may have unintended adverse consequences, such as deterring populations from using the new technologies, the erosion of human rights, or the creation of disparities in industrial competitiveness or development.

41. The prominent role played by industry in developing and maintaining the technologies also makes the integration of public- and private-sector measures important. Private-sector interests generally support effective crime control, but their motivations, which tend to be commercial rather than political, and their methods, which are technical rather than legal in nature, must both be reconciled, and where possible integrated, with the domestic and international efforts of Governments.

D. The role of the United Nations

42. As part of the preparation for the Millennium Assembly of the United Nations, the Economic and Social Council was called upon to consider the role of information technology in the fields of development and international cooperation. It concluded that the development and spread of new information technologies was largely self-sustaining, but that the United Nations could assist the process in important ways.[22] These included assisting developing countries in keeping up with the new developments, in particular in regions or subject areas where market-driven developments were not likely to meet their needs, and assisting in the development of specific technologies that could bring social benefits, but that were not necessarily commercially viable. More generally, it concluded that the key role of the United Nations was in building consensus and partnerships among stakeholders in the process, including Governments, academic institutions and private-sector companies. The purpose of the consensus-building was to assemble the necessary expertise and resources to ensure that everyone will have access to, and the opportunity to benefit from, the new information technologies.

43. High-technology and computer-related crime represents a significant obstacle to both access to and the potential benefits from what the Council described as a knowledge-based global economy, and the task of consensus-building will be just as important in the area of crime control. There is already general agreement about the need for effective crime control measures among States with significant investments and reliance on the technologies, but that is only the beginning of the process. The development of specific measures will require the assessment and reconciliation of numerous economic, social, cultural and legal issues. The elaboration and implementation of many crime control measures will have to be supported by near-universal consensus and by adequate standards of technical

ability in virtually every country if they are to prove effective. The consensus should extend not only to countries and their Governments, but to large, multinational private-sector interests as well.

44. In the immediate future, it is important that accurate information about the nature and scope of the problem and the views of Member States about what should be done to address it should be assembled and disseminated to permit States to consider options and give direction to the United Nations as to how it should proceed. The intergovernmental organizations described in the present report, as well as some individual Governments, have already begun the process of sharing the legislative, prosecutorial, technical and law enforcement expertise that they have developed with other States, both in general and in the context of individual cases of major transnational crime. That should be expanded, both in scope and in the number of countries involved, but to do so, an accurate assessment of existing needs and of the resources available to respond to those needs will be required.

45. It is therefore recommended that the Centre for International Crime Prevention of the Office for Drug Control and Crime Prevention of the Secretariat be directed to conduct a more detailed study of the problem, for submission to the Commission on Crime Prevention and Criminal Justice at its eleventh session. Possible subject matter for the study will be further discussed below, but it should include at least a survey of the basic needs of Member States, their willingness to assist through the provision of financial resources and technical expertise and their views as to how a global response to the problem should be developed and what form such a response should take.

46. It is further recommended that an open-ended intergovernmental group of experts be established to review the study and to prepare options and recommendations for further consideration and action by the Commission at its eleventh session. As noted above, the participation of a full range of countries is important at all stages of the process. It is important that this Group be as broadly based as possible, and in particular that it include representatives of developing countries. It is therefore recommended that such participation be supported by voluntary contributions from other States to the greatest extent possible.

47. It is further recommended that a global programme against high-technology and computer-related crime be established once the study is complete and the views of the group of experts have been obtained, and that interested States provide voluntary contributions to establish and support such a programme. The recommendation is discussed in detail in section F below.

48. Over the longer term, many experts are of the view that nothing less than a comprehensive, global legal instrument against high-technology and computer-related crime will be sufficient to establish the policies, powers, procedures and mechanisms for international cooperation needed to deal effectively with transnational computer-related crime. Views are mixed, however, as to how quickly such an instrument can be developed. As noted in section B above, there is a need to involve a wider range of countries early in the process. There are also major issues that would have to be resolved in drawing up such an instrument, for example, issues relating to national sovereignty, the application of judicial and other human rights safeguards and the role of private-sector interests in measures to promote computer security and crime control. Those issues must be taken into consideration in assessing options, both for the process of drawing up an instrument and for its possible form and content. In general, an instrument containing more extensive and binding provisions would be more effective, but would take longer to negotiate and prove more difficult and time-consuming for many States to implement. No conclusions can be drawn at the current stage, but it is recommended that the group of experts be asked to consider procedural and substantive options with respect to an international instrument and to develop recommendations as part of its report to the Commission at its eleventh session.

49. A further factor to be considered is the fact that high-technology and computer-related crime appears to be rapidly increasing in frequency, geographical scope and technical complexity, a process that seems likely to continue, in parallel to the rapid development and proliferation of new computer, network and telecommunications media. Such a prospect suggests that, while a global legal instrument may represent an important long-term response, effective measures in the more immediate future may also be needed. It is therefore recommended that the group of experts also be asked to develop further options for a global short-term strategy against high-technology and computer-related crime, focusing on areas such as general and case-specific legal and technical assistance; the setting

of technical standards for such things as the gathering, preservation, authentication and disclosure of electronic evidence; and the establishment of focal points or points of contact for requests for assistance. In that regard, work already under way in the organizations described in section II, subsection A, of the present report should be taken into consideration.

E. Elements of a detailed study

50. In the current state of knowledge, the field of computer-related crime still raises many more questions than answers, and further study is needed to define the subject matter, determine the interests it affects and how it affects them, and identify policy options for the future. The study should involve at least the following:

(a) The views of States about the nature and scope of the problem and possible domestic and international responses to it should be surveyed;

(b) States representing a full range of industrial, legal, social and economic characteristics should be consulted;

(c) Both domestic and transnational offending should be considered. While many States will see some issues as purely domestic concerns, the nature of the technologies breaks down traditional distinctions between domestic and transnational crime. Researchers, policy makers and negotiators will frequently find it difficult to distinguish between domestic and transnational offending, which argues for an integrated approach, in particular at the preliminary stages of the process;

(d) The views and assistance of private-sector elements should be included, with the following aspects highlighted:

(i) The study should examine and consider the views and input of the industries responsible for the development and operation of relevant technologies, including computer hardware and software and computer and telecommunications networks;

(ii) The study should also examine the views of relevant non-governmental organizations. Organizations dedicated to causes such as freedom of expression and the protection of individual privacy have been critical of previous attempts to develop effective investigative powers and have generated political opposition to the efforts of the Group of 8 and the Council of Europe in that area;

(e) The study should consider matters outside crime control, such as sustainable development, the protection of privacy, freedom of expression and other basic rights, as well as commercial and other interests. Those fundamental interests and others are closely linked to technological development, and they are likely to be affected both by increases in computer-related crime and by efforts on the part of Governments and the international community to prevent and control it;

(f) The study should assess the extent of offending, both generally and in the context of statistically relevant factors, such as specific forms of criminality, geography and other social or economic conditions. The difficulties in the gathering and analysis of accurate statistical information have already been examined. As a common understanding of the technical scope of the field and of the typology of offences within it is developed, however, more reliable data should become available. Further, with increasing popular awareness of the types of conduct involved and of the fact that they are, or should be, treated as crimes, the underreporting of such crimes should be reduced. The gathering of preliminary data is also important to building political support for effective domestic and international action against such crimes;

(g) The study should consider the definition and classification of high-technology and computer-related crime. The classification used in the present report is consistent with other work in the field and may serve as the basis for further consideration, but a more thorough and rigorous examination is needed to produce a framework that would enjoy consensus among Governments, interest groups and experts in the field. That is an early priority, as definitions and classifications are needed to bring consistency to the gathering of statistics and research on which further policy development will be based. A viable typology will require the consideration of factors in several major areas, including the following:

(i) *The relevant technologies.* The field of high-technology and computer-related crime is driven to a large degree by the nature and scope

of the technologies involved, which are rapidly evolving and converging. For that reason, the generic phrase "high-technology and computer-related crime" has been used in the present report and in other work on the subject. Research is needed to survey the full range of technologies involved and propose options for a general classification that would include all of them. More detailed consideration of specific technological developments and the types of criminal activity that depend on them is also needed. Given the rapid evolution of the technologies, consideration should be given not only to current technologies, but also to potential developments;

(iii) *The nature and motivation of offenders.* Offenders who commit crimes created by the new technologies represent a relatively new area of study. The motivations of more traditional offenders such as paedophiles, perpetrators of fraud or international drug-traffickers are well established. The adaptation of such offenders to the new technologies requires examination from the perspective of computer-related crime;

(iii) *Geographical aspects of offences.* The geographical aspects will differ from those of more conventional offences in at least two major respects. The first is that two major "geographies" are superimposed on one another. The actual physical location of offenders and its specific situational factors, such as the social, economic or cultural conditions, will be important. Also important, however, will be the electronic geography—the much-cited cyberspace considerations—that affect offending patterns.

F. Options and specific recommendations for further work on high-technology and computer-related crime

1. A possible international instrument against high-technology and computer-related crime

51. Once a study has been completed, it is recommended that the group of experts advise the Commission on the issues and options relating to whether it is feasible and desirable to draft up an international instrument against high-technology and computer-related crime. These issues will include the following:

(a) The question whether an instrument, if any, should be normative or legally binding. An instrument could seek to establish mandatory requirements for such things as criminal offences, investigative powers and mechanisms for international cooperation, or it could merely provide guidelines to assist States in developing effective measures and to promote international standardization of laws and procedures. A compromise between those two options, illustrated by the United Nations Convention against Transnational Organized Crime, would involve an instrument in which some provisions created binding obligations, while others contained more general guidelines or left implementation to the discretion of States parties;

(b) What relationship, if any, a further instrument would have to the United Nations Convention against Transnational Organized Crime. Generally, the Convention might serve as a precedent for some provisions, while others may not be appropriate for the subject matter of high-technology and computer-related crime. The limitation of the scope of the Convention to the activities of "organized criminal groups", for example, would exclude a significant proportion of high-technology and computer-related offences, because such offences are committed by individuals or groups that are not within the terms of the definition set forth in the Convention.[23] The possibility of drawing up a further protocol to the Convention for offences of that type therefore seems to be precluded;[24]

(c) How an instrument, once concluded, could be kept up to date. As noted in the introduction to the present report, the field under consideration is characterized by dynamic evolution of the technologies and related criminal activities, and it will be important to ensure that any framework for integrating domestic and international measures can keep pace with the changes. Options may include the delegation of some legislative powers to a body of experts representing the States parties and established for that purpose, the use of Protocols to deal with new specific issues as they arise, the use of relatively broad, technology-neutral drafting or other measures;

(d) How to incorporate related interests such as privacy, freedom of expression and other human rights and commercial interests into an international instru-

ment. While the subject matter requires that the focus of an instrument be on the control and prevention of crime, those other interests must also be considered, both in the process of drawing up an instrument and in its substantive content.

2. A short-term strategy for dealing with high-technology and computer-related crime

52. As noted above, high-technology and computer-related crime is a pressing problem that may require a concerted international response in both the short and the long term. It is recommended that the study review possible measures that could be taken in the immediate future, and that the group of experts develop recommendations regarding a short-term strategy for consideration by the Commission at its eleventh session. The elements of such a strategy may include the following:

(a) The compilation and dissemination to all Member States of information about high-technology and computer-related crime and possible responses to it, in order to inform, as quickly as possible, those not already engaged in discussions. The proposed study would form a key element of information packages, but other materials are also available, including the following:

(i) The *United Nations Manual on the Prevention and Control of Computer-related Crime*, published in 1994, could be updated and reissued;

(ii) The proceedings of and material from the workshop on crimes related to the computer network, held at the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, could be published and disseminated;[25]

(iii) Material from other intergovernmental organizations, in particular the Council of Europe, Interpol and the Lyon Group established by the Group of 8, could be disseminated more widely;

(iv) Workshops, seminars or briefing sessions could be held with officials of interested States, with the possible participation of representatives from the private sector;

(b) Material relating to the training of investigators and prosecutors could be made more available. The United Nations has not produced such material, but a number of Member States have done so for use in training their own officials, and in some cases for use in technical assistance projects involving other States;

(c) Direct technical assistance will be needed in some States. Such assistance may include training for judges, prosecutors, investigators and technical or forensic experts, many of whom would then be in a position to train others. In some cases, such projects may be integrated with more general development projects aimed at assisting States in acquiring and using new technologies for development. As noted above, it will be important that crime prevention and control become established as an integral part of such projects if the adverse effects of computer-related crime on development are to be avoided;

(d) The establishment of focal points or points of contact in each Member State should be encouraged. That would include points of contact for immediate assistance in computer-related crime investigations,[26] but also more general contacts for the purpose of gathering information about developments in each State and for receiving and disseminating information from the international community;

(e) A substantial commitment of financial and technical resources will be needed. Such assistance may take the form of voluntary contributions to the United Nations Crime Prevention and Criminal Justice Fund or the furnishing of expertise or materials to support a global programme against high-technology and computer-related crime or specific United Nations projects. The universality of the technologies and their vulnerability to exploitation by offenders anywhere provide incentives for States with financial or technical resources to assist other States. The industries that develop and operate computer and telecommunications networks also have financial and technical resources that can be tapped, as well as incentives to contribute, because many forms of computer-related crime threaten the commercial viability of their products.

3. The establishment of a global programme against high-technology and computer-related crime

53. The available evidence indicates that there is a considerable amount of activity in research and in the

development of policy, legal and technical measures, but little overall coordination of such activities. The extent of activity varies from country to country. It involves a number of intergovernmental and non-governmental organizations as well as several agencies and departments of the United Nations, and is a major concern for commercial companies and non-governmental interest groups. Attention, as well as the allocation of resources, tends to focus on specific issues of concern to the Governments or organizations directly involved, raising the potential for gaps or inconsistencies in research. The global nature of the United Nations places it in a unique position to examine and coordinate activities in the area under consideration. It is recommended that, once the needs and views of Member States have been surveyed, a global programme against high-technology and computer-related crime be established. It is also recommended that concerned States provide voluntary contributions to set up and operate such a global programme.

54. Possible terms of reference for the global programme should be considered by the Commission at its eleventh session, once the results of the study and the views of the group of experts have been obtained. The mandate of the global programme may include the activities set out in paragraph 52 above, as well as the following:

(a) The identification of Member States requesting assistance and the analysis of their specific needs;

(b) The development of materials to assist policy makers, legislators, law enforcement agencies, prosecutors and other relevant officials in dealing with domestic and transnational cases;

(c) The assembly, compilation and dissemination of materials prepared by others;

(d) The delivery of legal, technical and other assistance to States that request it, subject to the availability of sufficient resources;

(e) The development of an inventory of technical expertise available from individuals and agencies willing to provide assistance to requesting States;

(f) Coordination of activities with other agencies and departments of the United Nations, in particular in the areas of human rights and development, with a view to including the subject of computer-related crime in other programmes, where appropriate, and ensuring that input from other programmes is incorporated into the development of strategies for crime prevention and control;

(g) Coordination of activities with other intergovernmental organizations and individual Governments and agencies active in the area of high-technology and computer-related crime;

(h) Coordination of activities with non-governmental interest groups and private-sector companies and the organization of monetary resources and technical expertise from companies as part of a global strategy against high-technology and computer-related crime.

4. A preliminary inventory of substantive issues for consideration

55. As elements of both short- and long-term strategies, many of the same substantive issues will have to be addressed. On the basis of previous deliberations in the United Nations and other forums referred to in the present report, the following substantive issues require consideration:

(a) The identification of harmful conduct involving new technologies and the creation of new offences or the amendment of existing offences to criminalize it;

(b) The development of principles for dealing with the transnational tracing of communications, including powers to obtain, preserve and disclose traffic data;[27]

(c) The development of principles governing intentional and inadvertent cross-border electronic searches;

(d) The development of common principles for dealing with the interception of communications transmitted on computer networks and similar media;

(e) The assessment of the confidentiality or privacy interests inherent in various forms of data storage and transmission in order to develop procedural controls on seizure and interception in line with those interests. Most States place few, if any, restrictions on law enforcement access to open web sites or webcast communications, for example, but would apply restrictions to the seizure of data from more private sources;

(f) The development of common standards or practices for the identification of individual users of computer network or telecommunications services, balanced against the need for individual privacy and anonymity;

(g) The development of common principles for adjusting forensic practices and legal rules of evidence to ensure that computer evidence can be preserved, authenticated and used in criminal proceedings;

(h) The development of common principles for the protection of basic rights, both in establishing international policies and measures against high-technology and computer-related crime, and in implementing such measures in specific cases;

(i) The development of common principles governing the confidentiality and integrity of data and the balancing or reconciliation of those principles with the need for effective crime control measures;

(j) The development and funding of technical assistance programmes and materials for States that request such assistance. Such programmes and materials will be needed both to assist States in participating effectively in the development of global policies, and to ensure that domestic authorities are adequately trained and equipped to be able to respond effectively and expeditiously to requests for assistance in the investigation of transnational computer-related crimes;

(k) The gathering, analysis and sharing of information about new technological developments, offenders and their techniques and about effective methods of preventing, investigating and prosecuting offences;

(l) The training, equipping and resourcing of law enforcement experts to ensure the ability to investigate and prosecute effectively in domestic cases, and to be able to cooperate effectively with other States in transnational cases;

(m) The need to assess and clarify the role of the private sector and its relationship with Governments, both at the domestic and international levels. Specific elements or aspects of the relationship that will require consideration include the following:

(i) The need to strike a balance between effective crime control measures and the technical and commercial constraints on their development and implementation. Crime control should be considered by industries at the design stage of new technologies, but law enforcement must recognize that some measures may not be technically feasible or may represent changes that would render the technologies unproductive or uncompetitive. Crime control demands should not affect the basic viability or competitiveness of new technologies, but costs of crime and crime prevention must become part of the overall cost-benefit assessments of both Governments and industries, and costs should be allocated, where appropriate, against the profits generated by the technologies that support the crimes;

(ii) The need for Governments and industries to cooperate effectively to maximize the benefits and minimize the costs involved. That includes identifying and developing effective security and other crime-prevention techniques, their incorporation into new technologies at the earliest possible stage of development and the training and preparation of law enforcement and prosecutorial agencies with respect to new technologies before potential offenders gain access to them. The technological advancement of relevant industries makes them important for, if not essential to, the success of technical assistance programmes, and the commercial interests of the industries themselves will in many cases justify participation in such programmes;

(iii) The need to develop systems and conduct operations in ways that support effective criminal investigation and crime prevention, having regard also to the need to protect the privacy and other rights of users of the technologies. Examples include the operation of systems that can retain evidence of communications for reasonable periods, should it be needed for an investigation, and the need to be able to identify customers;

(iv) The need to develop a global assessment of the potential role of the private sector in crime control. That is a complex issue already facing many service providers, who share the public interest in effective crime control, but recognize the dangers and difficulties that arise if they become a substitute or replacement for State law enforcement agencies. Industries face conflicting pressures to incorporate security measures into

new technologies that may not be commercially viable, or that affect the fundamental interests of their customers.[28] They also face government pressures to control or exclude content seen as illegal or inappropriate, or to assist State law enforcement agencies in the conduct of criminal investigations. Those pressures raise complex ethical, legal and policy issues that should be explored, both at the national and global levels, with a view to achieving as much global consistency as possible.

Notes

[1] See "Building digital bridges" in the report of the Secretary-General to the Millennium Assembly of the United Nations (A/54/2000, paras. 150-167). See also the report of the Secretary-General on development and international cooperation in the twenty-first century: the role of information technology in the context of a knowledge-based global economy (E/2000/52, sects. III-V).

[2] European Committee on Crime Problems, Committee of Experts on Crime in Cyberspace, "Draft Convention on Cyber-crime" (PC-CY (2000), draft No. 25, rev. 5), available online at http://conventions.coe.int/treaty/en/projets/cybercrime25.htm.

[3] Conclusions from the studies are set forth in Council of Europe recommendations R (89) 9 and R (95) 13. The Committee of Experts was established by the Council of Europe Committee of Ministers at the 583rd meeting of the Ministers' Deputies, on 4 February 1997.

[4] See the annex to the communiqué of the Meeting of Justice and Interior Ministers of the Group of 8, held in Washington, D.C., on 10 December 1997.

[5] See the communiqué of the Ministerial Conference of the Group of 8 Countries on Combating Transnational Organized Crime, held in Moscow from 19 to 20 October 1999, para. 17 and annex 1.

[6] Meetings were held in Paris from 15 to 17 May 2000 and in Berlin from 24 to 26 October 2000. A further meeting is planned for Tokyo in May 2001.

[7] In paragraph 14 of resolution 1999/23, the Council requests the Secretary-General to conduct a study on effective measures that could be taken at the national and international levels to prevent and control computer-related crime, including an examination of the desirability of preparing manuals, guidelines and recommendations, and to report on the conclusions of the study to the Commission on Crime Prevention and Criminal Justice at its tenth session.

[8] See General Assembly resolutions 45/109 and 45/121 of 14 December 1990 and *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, 27 August-7 September 1990: report prepared by the Secretariat* (United Nations publication, Sales No. E.91.IV.2), chap. I, sect. C, p. 140.

[9] See A/CONF.169/16/Rev.1, paras. 370-385.

[10] See General Assembly resolution 55/25 of 15 November 2000, annex I, article 18, paras. 8 and 18.

[11] See *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders ...*, chap. I, sect. C.

[12] *International Review of Criminal Policy*, Nos. 43 and 44 (United Nations publication, Sales No. E.94.IV.5).

[13] See General Assembly resolutions 52/91 of 12 December 1997 and 53/110 of 9 December 1998. See also A/CONF.187/10 and *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 10-17 April 2000: report prepared by the Secretariat* (United Nations publication, Sales No. E.00.IV.8), paras. 161-174.

[14] See A/CONF.187/L.10, para. 14.

[15] See *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders ...*, chap. I.

[16] See articles 2 (use of terms) and 3 (scope of application) of the Convention (resolution 55/25, annex I).

[17] Such crimes were recently examined by the Financial Action Task Force on Money Laundering (FATF) of the Organisation for Economic Cooperation and Development (OECD). See the FATF "Report on money laundering typologies for 2000-2001" (Paris, OECD, February 2001), paras. 5-18.

[18] A/54/2000, para. 152.

[19] For example, the Director of the United States Federal Bureau of Investigation (FBI), in a statement on cybercrime to the United States Senate Judiciary Committee on 28 March 2000, reported that, from 1998 to 1999, the FBI caseload doubled from 547 to 1,154 cases, although it is not clear whether that was due to increases in offending or increases in reporting, or both. See also P. Graboski, "Computer crime: a criminological overview", *Forum on Crime and Society*, vol. 1 (2001), p. 40.

[20] Creation of the "Melissa" virus was admitted by a 31-year-old programmer from the United States. A 15-year-

old Canadian boy has pleaded guilty to 56 criminal charges in connection with the denial of service attacks. No charges have been laid in the case of the "I love you" virus, but it is believed to have originated in the Philippines. A wide range of damage estimates was circulated for each of those incidents, and the true costs will probably never be established. The figures are cited as evidence of the general scale of the losses and of the level of political concern about the threat posed by offences on such a scale.

[21] See E/2000/52, sects. III-V.

[22] See E/2000/52, paras. 79-99.

[23] See articles 2 and 3 of the Convention (resolution 55/25, annex I).

[24] The three existing protocols all incorporate the provisions relating to the scope and application of the Convention, mutatus mutandis. Many of the provisions of the Convention, having been drafted on the basis that they would apply only to cases involving organized criminal groups, would be difficult to apply to cases involving computer-related crimes committed by individuals.

[25] The United Nations Asian and Far East Institute for the Prevention of Crime and the Treatment of Offenders, which organized the workshop, is currently preparing those materials for publication.

[26] The process has already been started by the Group of 8 and followed up by Interpol.

[27] The term "traffic data" generally refers to the data stored by service providers that records the source and destination of an electronic communication. That may include both the ultimate source and destination and interim sources or destinations within a computer network. A related concept is "subscriber" or "user" data, which is used by service providers to identify individual customers.

[28] One recent example was an injunction by a French court requiring the Internet company Yahoo! Inc. to develop technical methods to block the access of its subscribers in France to auction web sites containing Nazi memorabilia. The sale of such items is prohibited in France, but legal in the jurisdictions in which the sites themselves are located. Providers are generally willing to take such action—to the extent that it is technically feasible—but only when a competent court or other public authority has determined that the content itself is illegal.